The Future of Privacy: Insights From the EU Digital COVID Certificate

Discussions about the use and security of personal data are ongoing. Questions include the future legal implications, emerging customer preferences and the effect of world events on privacy and security. One example is the need for European citizens to openly share their health information related to COVID-19 in a private and secure manner. The development of the EU Digital COVID Certificate (EUDCC) offers some insights into what the future may hold for managing individual privacy while supporting the effective use of information.

TILL MUELLER

Is a vocational training student at SAP SE, the market leader for enterprise resource planning (ERP) software. He has completed internships in several different areas, including application innovation services and technology and innovation.

GERALD F. BURCH | PH.D.

Is an assistant professor at the University of West Florida (Pensacola, Florida, USA). He teaches courses in information systems and business analytics at both the graduate and undergraduate levels. His research has been published in the *ISACA® Journal*. He can be reached at gburch@uwf.edu.

The COVID-19 Pandemic

The COVID-19 pandemic has greatly affected privacy and security. Once COVID-19 vaccines were approved in countries around the world, citizens needed to demonstrate compliance with local testing and vaccination protocols. During this time, reducing the spread of the virus was focused on limiting travel of those who could be contagious. Vaccinations and testing reduced the likelihood of COVID-19 illness and created a need for a secure way to check the COVID-19 status of each citizen.[1] The Israel Health Organization was the first to offer a solution when it developed the Green Pass, which displays a quick response (QR) code that stores information about an individual's health status. Other nations soon followed.[2]

One German state developed an application to display a QR code from a website where private data were hosted from a central server. Even though the process was encrypted at each step, data accuracy became an issue. Malicious actors were able to build a duplicate webpage that looked like the original to create QR codes, thereby providing a means to obtain false vaccination credentials.[3] The lesson learned is that digital vaccination records do not necessarily provide authorities with trusted data.[4]

EUDCC Development and the Legal Process

The process of developing a digital certificate became a balancing act of providing local authorities a means to allow people to safely move about the world (right of free movement) by accurately identifying COVID-19 vaccination/testing of individuals and simultaneously protecting individual privacy of health data. The Council of the European Union first issued recommendations on how to address the right of free movement within the European Union on 13 October 2020.[5] Just five months later (17 March 2021), the European Commission published a proposed framework for the Digital Green Pass[6] and stated that "in view of

the urgency, the Commission did not carry out an impact assessment."[7] This preliminary attempt was, therefore, suggesting that data privacy was secondary to data availability for authorities to manage the potential spread of the COVID-19 virus.

The European Data Protection Board and the European Data Protection Supervisor reviewed the recommendation and heavily criticized the proposal because it lacked privacy-related details, provisions and safeguards.[8] The proposal was amended on 21 May 2021 to include more privacy details and precautions. On 14 June 2021 the regulation was passed by Parliament, and on 1 July 2021 the first EUDCC could be issued.[9]

The development of the EUDCC is just one example of meeting government regulations while maintaining privacy.

Technical Background

The EUDCC uses a public-private key infrastructure with a common trusted authority. The job of this authority is to build trust by authorizing other entities to issue certificates in the name of the authority (European Union). The authority issues certificates to participating member states and approved countries, thereby allowing them to use the developed infrastructure to issue certificates to individuals.[10] For example, the German authority issued certificates to pharmacies and doctors who vaccinated individuals and to vaccination centers. This made it easy for individuals to convert their regular vaccination records into digital certificates based on vaccinations, tests or COVID recovery.[11]

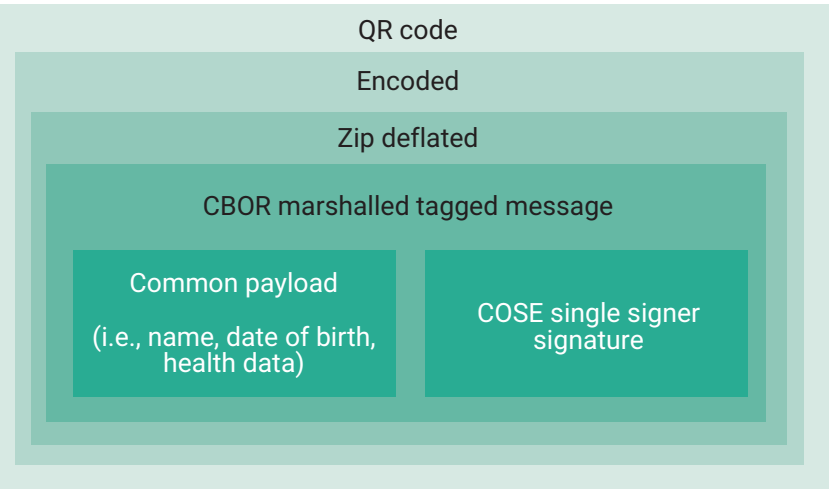
Certificates are displayed as QR codes based on text that is hashed and signed, making it readable by other machines and requiring no human input.[12] **Figure 1** shows the alphanumeric string stored in the QR code.[13] This string is encoded and zip-deflated to reduce storage. The Concise Binary Object Representation (CBOR) marshalled tagged message contains the personal data (common payload). Verification of the code is based on the CBOR Object Signing and Encryption (COSE) single signer signature, which provides assurance that the certificate has been issued by a trusted authority. Because the encryption process is open, technically, anyone can sign the COSE with their own private key.[14] Therefore, readers must verify the authority issuing the certificate. Most important, individuals' private data are saved in the QR code and are not stored in any central database or on any server.

In practice, the process follows these steps:

1. An authorized entity wants to check the COVID status of an individual.
2. The individual's QR code is scanned with the country's official application.
3. The application reads the information stored in the QR code, checks that it has been signed by a trusted authority and compares it to the country's current rules.
4. After a successful check, the authorized person verifies the name and birthdate of the person providing the QR code.

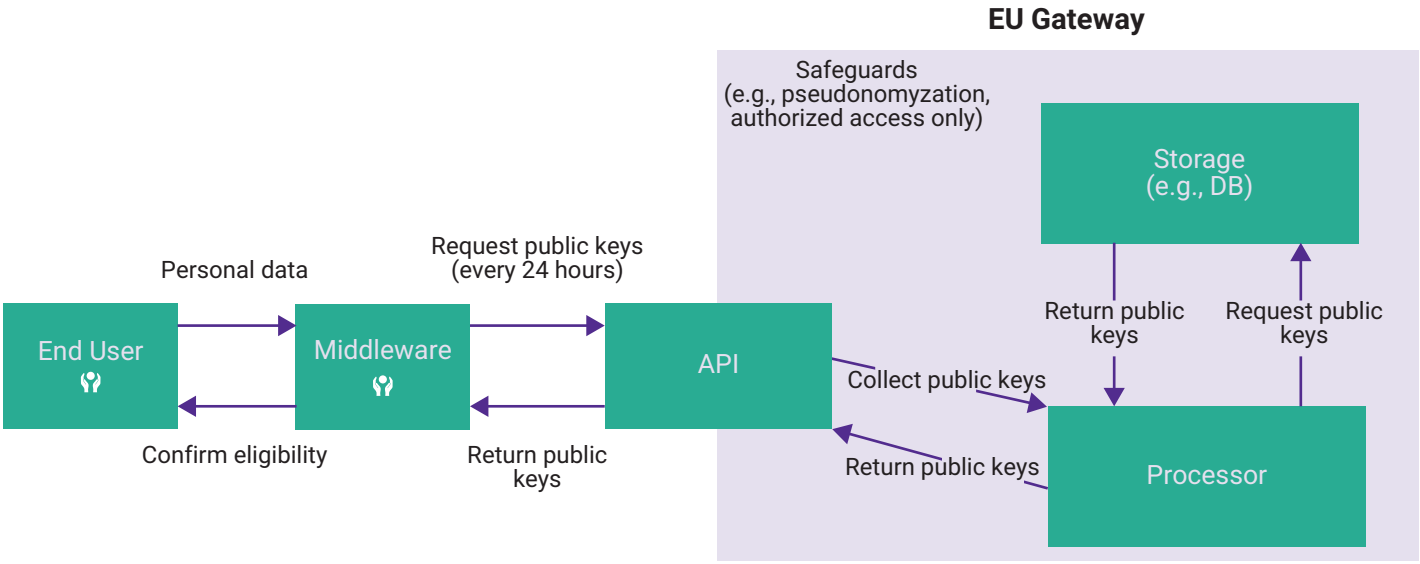
Figure 2 shows that personal data are stored with the end user, and only the public keys are maintained in a centralized system. The benefit is that the EUDCC is decentralized, and no personal data

FIGURE 1
EUDCC Technical Specifications



Source: Adapted from Leyrer, M.; "EU Digital COVID Certificate—Keine schwarze Magie" [EU Digital COVID Certificate—No Black Magic], Gulaschprogrammiernacht 20, 20 May 2022, *https://media.ccc.de/v/gpn20-10--eu-digital-covid-certificate-keine-schwarze-magie*

FIGURE 2
EUDCC Design



are communicated with a single entity or server.[15] However, allowing individuals to be responsible for their own private data does mean that loss of the QR code results in the loss of private data. In addition, anyone who knows how to decrypt the QR code (or middleware) can access the private data, so individuals must protect the QR code as they would any form of identification.

In the future, there may be less private data held in centralized servers and more held on personal devices that can be accessed only when and how the consumer chooses.

The Future of Privacy

The development of the EUDCC is just one example of meeting government regulations while maintaining privacy. Preparing for the future begins with looking at what organizations are currently doing to comply with regulations. The most common organization privacy strategy is to comply at the most minimal level, including maintaining a low profile, appointing data protection officers, asking customers for consent and providing roughly the same levels of privacy protection as competitors.[16] The development of the EUDCC suggests this level of compliance may no longer be the best approach for organizations. Government authorities may soon be requiring more privacy protection from organizations.

The EUDCC has been adopted by 27 EU states and 18 other countries,[17] thereby signifying the agreement of many countries on how to manage personal privacy, even during a crisis. Organizations must consider how government regulations affect the storage and processing of personal data. According to a recent report, 50 percent of the enterprises surveyed used the EU General Data Protection Regulation (GDPR) framework to manage privacy.[18] Even in the midst of the COVID-19 pandemic, the first version of the EUDCC was highly criticized by the European Data Protection Board for not adhering to more stringent privacy standards. Enterprises should see this as the wave of the future. Government regulations may continue to tighten practices related to the storage and use of public data.

Customer preferences are also beginning to change with regard to who owns their private data and how those data are used. In a 2019 survey of 2,601 adults worldwide, 32 percent of respondents said they were willing to switch service/product providers over data or data-sharing policies that potentially affected the individual's privacy.[19] People who hold these views have become known as privacy actives because they

are more willing to be vocal about privacy issues and to take actions based on an organization's privacy protocols. Privacy actives are typically young, affluent and shop online. An interesting aspect of privacy actives is that although they are concerned about the privacy of their data, they are willing to provide purchase histories in exchange for personalized products and services.[20] Therefore, it may be the case that consumers are more concerned with the transparency of what is happening to their private data. The EUDCC has shown that one way to manage this transparency is by allowing consumers to own and maintain their private data and control when and how other entities use those data. In the future, there may be less private data held in centralized servers and more held on personal devices that can be accessed only when and how the consumer chooses.

It may be time to stop trying to match competitors' privacy measures and to develop a competitive advantage by providing customers with more transparency and more control before government agencies require it.

A final consideration for developing privacy policies is the kind of technology that will be available in the future. One drawback of the EUDCC is the use of public vs. private keys. Currently, the EUDCC uses bar codes that are not encrypted. Therefore, data can be stolen by capturing an individual's bar code. This could be done on a larger scale by capturing all the bar codes scanned by one device, thereby gaining thousands of individuals' names, immunization statuses and locations. The development of private encryption keys that are activated when an individual presents digital identity credentials may not be too far in the future.[21]

Conclusion

The EUDCC has shown on a large scale the strengths and weaknesses of current technology and the governmental pressures exerted on enterprises to maintain individual privacy when creating processes that affect digital identity. However, the EUDCC is just one example signifying the growth of concern over individual privacy and current technology. Even during a time of crisis, the current expectations of governments and individuals lean toward more control over personal data privacy. Similarly, customers appear to be ready to choose product and service providers based on the use of their data.

Therefore, enterprises should consider which customer data they need to hold, how they use that data and with whom they share an individual's data. It may be time to stop trying to match competitors' privacy measures and to develop a competitive advantage by providing customers with more transparency and more control before government agencies require it.

Endnotes

1 Council of the European Union, Council Recommendation (EU) 2020/1475 on a Coordinated Approach to the Restriction of Free Movement in Response to the COVID-19 Pandemic, *Official Journal of the European Union*, Luxembourg, 13 October 2020, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H1475*

2 Gstrein, O. J.; "The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment," *European Journal of Risk Regulation*, vol. 12, 2021

3 Chaos Computer Club, "Vaccination Cards Do Not End Pandemics," 17 May 2021, *https://www.ccc.de/de/updates/2021/impfausweise-beenden-keine-pandemien*

4 *Ibid*.

5 *Op cit* Council of the European Union

6 European Commission, Proposal for a Regulation of the European Parliament and of the Council (Digital Green Certificate), Belgium, 17 March 2021, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130*

7 *Op cit* Gstrein

8 European Data Protection Supervisor, "EU Data Protection Authorities Adopt Joint Opinion on the Digital Green Certificate Proposals," 6 April 2021, *https://edps.europa.eu/press-publications/press-news/press-releases/2021/eu-data-protection-authorities-adopt-joint_en*

LOOKING FOR MORE?

- Read *Privacy by Design and Default: A Primer. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

9 European Parliament and Council of the European Union, Regulation (EU) 2021/953 of the European Parliament and of the Council (EU Digital COVID Certificate), *Official Journal of the European Union*, Belgium, 14 June 2021, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0953*

10 *Ibid*.

11 *Ibid*.

12 *Ibid*.

13 Leyrer, M.; "EU Digital COVID Certificate—No Black Magic," Gulaschprogrammiernacht 20, 20 May 2022, *https://media.ccc.de/v/gpn20-10--eu-digital-covid-certificate-keine-schwarze-magie*

14 *Ibid*.

15 *Op cit* European Parliament and Council of the European Union

16 Redman, T. C.; R. M. Waitman; "Do You Care About Privacy as Much as Your Customers Do?" *Harvard Business Review*, 28 January 2020, *https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do*

17 *Healthcare IT News*, "The EU Vaccine Passport Paves the Way for Digital Identity—But Pitfalls Lie Ahead," 14 February 2022, *https://www.healthcareitnews.com/news/emea/eu-vaccine-passport-paves-way-digital-identity-pitfalls-lie-ahead*

18 ISACA®, *Privacy in Practice 2022*, USA, 2022, *https://www.isaca.org/resources/white-papers/privacy-in-practice-2022*

19 *Op cit* Redman and Waitman

20 *Ibid*.

21 *Op cit Healthcare IT News*